REMARKS/ARGUMENTS

Claims 1-6, 8-20, and 22-28 are now pending in this application in light of the above amendments. Claims 1 and 15 have been amended. Claim 40 has been cancelled. The amendments find full support in the original specification, claims, and drawings. No new matter has been added. In view of the above amendments and remarks that follow, reconsideration, reexamination, and an early indication of allowance of the now pending claims 1-6, 8-20, and 22-28 are respectfully requested.

Claims 1-6, 8-20, 22-28 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. (U.S. Patent No. 6,769,063) in view of Windirsch (U.S. Patent No. 6,760,439) and further in view of Callum (U.S. Patent No. 6,320,964). Applicant respectfully traverses these rejections.

Claims 1 and 15, as amended, now recite "performing cryptographic operations on a data block, a first portion of the data block occupying a first position and a second portion of the data block occupying a second position," and "a two-level multiplexer circuitry including a multiplexer on a first level coupled to a multiplexer on a second level . . . wherein the multiplexer on the first level selects initial input data responsive to a first signal, and the multiplexer on the second level receives and associates, in response to a second signal, feedback data from a previous round of cryptographic processing, with the second position, for a next round of cryptographic processing." None of the cited references teach or suggest this limitation.

The Examiner acknowledges that Kanda does not disclose a "two-level multiplexer circuitry." However, he relies on Windirsch to make up for this deficiency. In doing so, the Examiner relies on the disclosure in Col. 1, lines 35-47 of Windirsch which discloses a "first multiplexer device" and a "second multiplexer device" connected via an XOR. The "second multiplexer" is depicted in the figure with reference number 13. This multiplexer selects one of two available input signals, one of which is a constant value and the other is provided by a first register 15 or a second register 17. (Col. 3, lines 58-62). Nothing in Windirsh teaches or suggests, however, that the disclosed second multiplexer "receives and associates, in response to a second signal, feedback data from a previous round of cryptographic processing, with the second position, for a next round of cryptographic processing" as is required by claims 1 and 15. Accordingly, claims 1 and 15 are now in condition for allowance.

Claims 2-6, 8-14, 16-20, and 22-28 are also in condition for allowance because they depend on an allowable base claim, and for the additional limitations contained therein.

Claim 40 has been canceled.

Appln No. 09/892,240
Amdt date August 29, 2005
Reply to Office action of June 29, 2005

In view of the above amendments and remarks, Applicant respectfully requests reconsideration, reexamination, and an early indication of allowance of the now pending claims 1-6, 8-20, and 22-28.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By ______________________
Josephine E. Chang
Reg. No. 46,083
626/795-9900

JEC/lal
AB PAS633352.1-*-08/29/05 3:49 PM